Amendments to the Specification

Please amend the Specification as follows:

Page 5, Line 22, please replace the paragraph that starts "■ E = $\{0.1\}^6$ and F = $\{0.1\}^4$" with the following new paragraph:

■ ~~E = $\{0.1\}^6$ and F = $\{0.1\}^4$~~ E = $\{0,1\}^6$ and F = $\{0,1\}^4$

Page 5, Line 27, please replace the paragraph that starts with "■ f' is built as follows" with the following:

■ f' is built as follows: if x is an element of E' (therefore on 6 bits), the first bit and the last bit of f'(x) are those of x; the four bits in the middle are those given by the usual result of the boxes. A brief analysis of the operating mode used with the S boxes shows that for all elements of E we have: ~~$h_2(f'(h_1(x))$ = S-box(x)~~ $h_2(f'(h_1(x)))$ = S-box(x). Concerning the verification function, it is first used on the results output from each round (64 bits) and on the concatenated outputs of the function f' (48 bits which will be considered as 64).

Page 7, Line 20, please replace the paragraph that starts with "Sometimes" with the following paragraph:

Sometimes, the attacker does not control the error introduction fully. By working on a larger space and by checking the consistency of the results, an error introduced can therefore be detected since it generates an impossible result. For example, if two eight-bit numbers are added and the result is stored on 16 bits, an error introduced on the result has a strong ~~change~~ chance of affecting the 7 most significant bits (generally 0 using the laws of arithmetic) which means that the error will be detected.